Chapter Eight Table of Contents

Security Education, Training, and Awareness Plan

All DPAS personnel receive annual security awareness training. DPAS personnel who are part of the Implementation and Training Team receive an Anti-Terrorism Briefing. Users of DPAS receive this Security Awareness Guide, which explains appropriate measures to safeguard the system.

Each agency and service employing DPAS has the responsibility to ensure that their personnel comply with the DPAS Security Awareness Guide and receive annual security awareness training as well as any required technical training as needed.

Preface

This document prescribes the security policy and associated security requirements applicable to the DPAS. It applies to DPAS implementations and defines the rules governing the protection of DPAS data, services, resources, and security services associated with DPAS applications and processes. The implementation and operation of the DPAS must support the complete and consistent enforcement of this security policy.

This security document defines a minimum set of rules to be enforced for the protection of data, services, and resources under DPAS cognizance. Local security authorities may apply more stringent rules or constraints, while not degrading the DPAS security posture and maintaining consistency with the minimum essential required security rules identified in this DPAS Security Policy.

The guidelines described in this document provide a set of good practices related to the use of password-based user authentication mechanisms in automatic data processing systems employed for processing non-classified sensitive information.

Continued security training and the introduction to security awareness for new employees are the responsibility of the local site. Security refresher training should also be required when personnel assume new or different duty responsibilities, when significant configuration changes occur that affect security or when different threats or new vulnerabilities are identified.

Application security training is given in DPAS User Training Basic and Basic Plus courses and is provided upon request. This training addresses topics such as security set up, roles and responsibilities and segregation of duties.

Security Awareness

EXECUTIVE SUMMARY

Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, Appendix III, Security of Federal Automated Systems, requires that Federal agencies provide an adequate level of security for all agency Automated Information Systems (AIS) to assure that automated systems operate effectively and accurately, that the appropriate physical, personnel, administrative, and technical controls are implemented, and to assure continuous operation of automated systems that support critical agency functions. DoD Instruction 8500.2, *Information Assurance (IA) Implementation*, and DoD 8510.1-M, *Application Manual, Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP)* provides the mandatory, minimum AIS security requirements which must be enforced.

DPAS is dependent upon AISs and computer resources to perform its mission. To protect these resources, DoDI 8500.2 and DoD 8510.1-M mandate the implementation of an AIS security program. The requirements of the AIS security program are to develop an AIS security plan, perform security testing, and prepare a certification package. This Security Awareness Guide (SAG) is part of the DPAS security program documentation.

INTRODUCTION

The purpose of this Security Awareness Guide (SAG) is to explain how the security features of the DPAS work and to provide other user relevant security information. This will allow users to consistently and effectively protect their information. The SAG is written for the users of the DPAS application and will provide users with the necessary security information to correctly use the protection features provided by the system. This SAG will give users the appropriate security information that is required to enter the DPAS system and securely process information.

SYSTEM SECURITY OVERVIEW

All data processed and transmitted via the DPAS has been categorized as being sensitive unclassified. The purpose of determining the types of sensitivity of data to be processed is to assist in the selection of appropriate protection services and mechanisms. All Government information requires some level of protection of confidentiality, integrity, and availability. Information that an adversary places value on will require some kind of security protection. Data identified as Sensitive But Unclassified (SBU) must be provided protection at the C2 level of protection.

Data Protection Objectives

The two major objectives for protecting data processed by the DPAS are to (a) ensure that data is protected from unauthorized modification and disclosure during preparation and transmission of DPAS information and (b) ensure data integrity is provided during transmission.

Risks. A Risk assessment for the DPAS system has been completed. The findings of this risk assessment have been used in selecting and implementing the security measures for the DPAS. Risks to the security of DPAS can be divided into those which arise from potential malicious action, from accidents or improper procedures, and from loss of assurance that the system can function as designed and provide the requisite protection.
Risks from malicious action include:

- Unauthorized origination of transactions;
- Intentional alteration of transaction contents after origination;
- False claim of transaction loss between sending and receipt;
- Attacks on the key management infrastructure;
- Unauthorized receipt, interception, copying or viewing of sensitive information; and
- Malicious software replacement or database corruption.

Risks from accidents or improper procedures include:

- Inadvertent or other unauthorized origination of DPAS data;
- Real transaction loss or mistaken claims of transaction loss;
- Mistaken claims about times of transaction events;
- Accidental software replacement or database corruption; and
- Natural disasters.

Threats and Vulnerabilities. DPAS is vulnerable to many threats that can inflict various types of damage resulting in significant data/information losses. Damage can range from errors that will effect the database integrity to fires that can destroy the entire computer center. Losses can stem from actions of supposedly trusted employees defrauding a system, from outside hackers, or from careless data entry clerks. The effects that threats can have on the DPAS varies considerably with some affecting the confidentiality or integrity of data while others affect the availability of a system.

Listed below are some of the threats that could affect the DPAS environment.

1. **Errors and Omissions.** These are errors and omissions caused by data entry clerks or by all types of users who create and edit data.
2. **Fraud and Theft.** The exploitation for both fraud and theft by "automating" traditional methods of fraud and by using new automated methods.
3. **Employee Sabotage.** Exploitation of the DPAS by employees.
4. **Malicious Hackers.** Sometimes called crackers; this term refers to those who break into computers without authorization for the purpose of doing some type of damage to the application or system. This term can include both insiders and outsiders.
5. **Espionage.** The act of gathering proprietary data/information from private companies or the government for the purpose of aiding another company. Companies or governments can perpetuate these intrusions.
6. **Malicious Code.** This term refers to viruses, worms, Trojan Horses, logic bombs, and other uninvited software.

7. **Foreign Government Espionage.** Threats posed by foreign government intelligence services. Foreign intelligence services may target unclassified systems to further their intelligence missions.

8. **Threats to Personal Privacy.** The accumulation of vast amounts of electronic information about individuals by governments, credit bureaus, and private companies, combined with the ability of computers to monitor, process, and aggregate large amounts of information about individuals have created a threat to individual privacy.

9. **Loss of Physical and Infrastructure Support.** Loss of supporting infrastructure includes power failures, loss of communications, water outages and leaks, sewer problems, lack of transportation services, fire, flood, civil unrest, and strikes.

User Protection Guidelines. It is a user's responsibility to protect sensitive government information. Users should always be cognizant that sensitive and mission-critical information requires protection from disclosure, alteration, and loss. Information protection guidelines are listed below:

- **Protection of Equipment.** Users must keep food, drink, and electrical appliances away from their workstation and magnetic media (diskettes).

- **Protection of User Work Area.** Users should always be aware of who is in their area and challenge and assist personnel who do not belong in the area.

- **Protect Passwords.** Use only permitted passwords and do not share passwords with anyone; change passwords regularly.

- **Protection of Files.** Assign access protection to each sensitive file. Periodically review access privileges for each sensitive file.

- **Protection of Workstation When Unattended.** Users must always logout when leaving their terminals unattended or "lock workstations", requiring the entry of the password before the workstation can be used.

- **Protection Against Viruses.** Users must never bring unauthorized or personal software to work. Users must apply anti-virus updates as directed. Users must not open e-mail of a suspicious nature. Users must not open attachments if they are not work related or are from an unknown source.

- **Protection of Sensitive Magnetic Media.** All sensitive removable magnetic media and equipment must be locked up when not in use.

- **Protection Against Disaster.** Always have back-up programs, equipment and databases stored at an off-site location. Each user must store their work files in the "backup" directory and execute the back-up process regularly.

DPAS Users Will:

1. Access the DPAS only when formally authorized to do so and only for authorized purposes.

2. Not disclose, lend, or otherwise compromise their personal authenticators (passwords) and promptly report any suspected compromise of their or any other authenticator to their Terminal Area Security Officer (TASO) or Information Awareness Officer (IAO).

3. Be responsible for adhering to the DPAS Security Policy and DPAS Security Awareness Guide. Deliberate failure to obey security provisions of these policies may result in disciplinary action.

4. Use only Government-purchased or Government-approved software in the conduct of official Government business.

5. Notify the TASO or IAO when access to the DPAS is no longer required or has changed due to job reassignment or termination.

6. Attend the initial security training as coordinated by the TASO or IAO, prior to accessing the DPAS. Participate in the security awareness program and in the annual refresher security training provided by the DPAS.

7. Protect the DPAS data and resources from unauthorized disclosure, modification, or deletion.

8. Change their password when instructed by the system or security documentation.

9. Use anti-viral software installed on their system. Scan all software for viruses prior to initial use.

10. Not install or use privately owned, personally developed, public domain, or shareware software on the DPAS system.

11. Notify the TASO and/or the IAO of suspected or confirmed virus attacks.

12. Protect from unauthorized view the entry of their password or the display of sensitive unclassified data that resides on the workstation.

13. Comply with DoD and the DPAS security policies on the use of the Internet, downloading of files, and e-mail.

14. Not modify or change the hardware or software configuration of their workstation by adding unapproved hardware or software.

15. Not bypass any surge protection or power line conditioning devices installed on their system.

16. Address security questions to their supervisor, IAO, or TASO.

DPAS Security Protection Requirements. Users should assure that they always use the security features built into the DPAS system. Users should never attempt to bypass DPAS security features. If users believe that these security features are not adequate for the protection of sensitive but unclassified information, they should notify their Information System Security Officer (ISSO) or their TASO.

System Philosophy of Protection

The DPAS security controls require that each activity's data be stored in a uniquely identified database. Access to the DPAS icons and programs are restricted according to the user's specific property accountability duties and their "need to know". Each user requiring DPAS access will be provided a unique logon ID, password, and a database/site ID name(s). DPAS is divided into the following applications: Document Register, Authorization, Catalog, Accounting, Hand Receipt, Hand Receipt Holder, Maintenance and Utilization, Inquiries, Ad Hoc Reports, Utilities, and Security modules. Within each application are related programs that support the related business function of the applications. Some programs provide update and delete functions/operations, while other programs provide read only functions. DPAS has been determined to contain only sensitive-unclassified data.

The data contained in the unique DPAS database is owned by the applicable DoD organization and therefore is the responsibility of the DoD organization to insure the accuracy and integrity of the data being maintained. DPAS was designed to operate in a client-server Windows based environment, with the server executing under UNIX. The DPAS includes real time updates, and utilizes the features of CINCOM's SUPRA database management system and Eureka Client commercial software. DPAS resides at the Defense Enterprise Computing Center-Ogden (DECC-O) in Utah. All users of the system are required to have a unique logon ID and password to sign on to the DPAS. Password rules and user's responsibilities are detailed in the Security Related Commands for Using DPAS section of this manual

Security Officials

The Security Administrator. The Security Administrator is a person designated at DECC-O to establish user accounts to access DPAS. This user has a UNIX login and is responsible for managing the UNIX environment that DPAS exists in. This person designated at the DECC-O establishes user accounts (logon Ids, passwords, database ID) to access DPAS.

If an Accountable UIC Security Officer or a Database Security Officer is assigned at a site, he/she can also establish DPAS user accounts. However, they are only allowed to establish accounts for their assigned accountable UICs or Databases respectively. If a site does not have an assigned Site Security Officer, the site will be required to request access from the Security Administrator for all users needing access to DPAS in the normal performance of their assigned duties. The Security Administrator will also be responsible for removing users from the system who no longer need access, reset passwords, and serve as the focal point for any security related matters that may affect the users ability to access DPAS. The Security Administrator accomplishes these tasks by accessing DPAS with a special security login that will only give him/her the Security module. See **Security Responsibility** Table for security responsibilities.

Information Assurance Officer (IAO). This user, if assigned, will reside at the site and may also be referred to as a Site Security Officer. This user cannot add or delete any system users. This user can change the name, phone number, e-mail address, password and suspension date for an end-user with the same accountable UIC. This user can change name, phone number and e-mail address for another site/database-level security user. This user can modify the DPAS module and program access profiles for end-users. This user cannot add or delete users. The IAO accomplishes these tasks by accessing the DPAS with a special security login that will give him/her only access to the Security module. This user's DPAS Security account must be established by the Security Administrator at DECC-O.

Site Security Officer. Term used throughout this document to refer to the Accountable UIC Site Security Officer, and the Database Site Security Officer. In some cases, this may also be the Information Assurance Officer (IAO) or the Terminal Area Security Officer (TASO). The Accountable UIC Site Security Officer is a person designated at the users site or agency. This user cannot add, modify, or delete any end-users with the same accountable UIC. This user can modify the DPAS module and program access profiles for the end users. The Site Security Officer accomplishes these tasks by accessing DPAS with a special security login that will give him/her only access to the security module. The Database Site Security Officer is a person designated at the user's site or agency that can add, modify, or delete any end-users to their database at the agency. This user's DPAS Security account must be established by the Security Administrator at DECC-O.

User Security Responsibilities

All DPAS users are responsible for the accuracy and integrity of the data residing on the site's database. Some users will have the responsibility for adding, updating, and deleting data in the database, whereas others may only be able to read the data. Engaging in experimentation with the DPAS programs is discouraged. Events that alter data in the database are subject to audit. Each user will be provided a unique logon ID and password, as well as a site database name, and a list of the DPAS icons and programs that can be accessed. It is the responsibility of the user to safeguard their logon ID and password against accidental disclosure to persons not authorized to access DPAS. *It is the responsibility of the Security Administrator and/or the Site Security Officers to ensure that they use the Discretionary Access Features built into the DPAS system. At no time should users be given access to processes they have not been authorized to use*.

USING DPAS

The following outlines the security features for using DPAS. If problems logging on to DPAS are experienced, contact the designated Site Security Officers (e.g., IAO, Database Site Security Officer, Accountable UIC Site Security Officer, Terminal Area Security Officer) or the Security Administrator (DECC-O), or Help Desk Columbus for assistance.

a. The user's immediate supervisor must request DPAS access. A DPAS logon ID, password, and site ID/database name will be requested from the Site Security Officer or Security Administrator. The Site Security Officer or the Security Administrator at DECC-O will connect the logon ID to the required icons and programs, and provide the logon ID; password, site ID/database name, and a list of the icons and programs as assigned to the user.

b. The DPAS Desktop displays all of the icons and programs that are available within DPAS. Access to the icons and programs depend upon the assigned duties. If an icon or program is not authorized, it will be grayed out.

c. The security provided by a password-protected system depends on the passwords being kept secret at all times. Thus, a password is vulnerable to compromise whenever it is used, stored, or even known. In a password-based authentication mechanism implemented on an ADP system, passwords are vulnerable to compromise due to poor security habits by users. This guide prescribes steps to be taken to minimize the vulnerability of passwords in this circumstance.

The following rules apply to all users accessing DPAS:

(1) **Keep Passwords Confidential**

- **DO NOT SHARE** logon ID and/or password
- **DO NOT** write it down or discuss it[1]
- **DO NOT** recycle previously used passwords
- **DO NOT** attempt to change the password more than once a week. After one week, passwords may be changed as often as desired, it is not necessary to wait until the expiration date
- **DO NOT** create a password that is the reverse of your logon ID.
- Select a password known only to you
- Memorize the password

[1] DoD Password Management Guidelines CSC-STD-002-85

(2) **Be Careful, Conscientious and Responsible**

- When signing on to DPAS
- When updating information

(3) **Be Data Security Conscious**

- Protect your password from disclosure
- Prevent against its misuse
- Protect the integrity of the data
- Do not use common dictionary words
- Do not use your name or any part of your name, etc.
- Use a minimum of 8 and a maximum of 12 alphanumeric characters in length and must contain 2 of the following 3: a capital letter, a numeric or special character (only @, #, $, underscore). However, the first position cannot be an underscore

(4) **Do…**

- Follow established logon procedures carefully
- Be diligent when entering/inputting information/data

(5) **Don't**

- Reveal, disclose or share your logon ID/password/access privileges
- Leave terminal unattended when logged on
- Engage in system experimentation

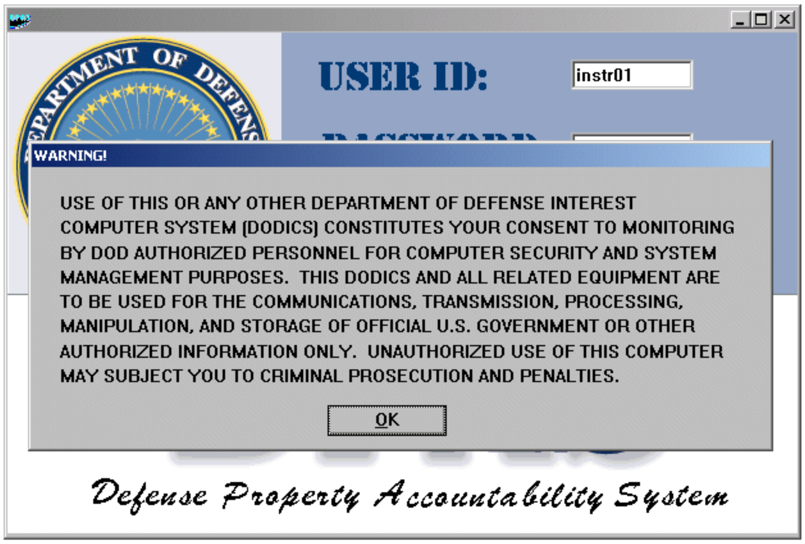
Security Related Commands for Using DPAS

The following sections will provide step-by-step instruction on how to log on to DPAS, change passwords, log off, explain error messages and their causes, explain the access controls, and audit trails. Since the intent of this document is to educate and guide the user to the proper ways of utilizing security controls, "how to" information for data manipulation is not addressed, but is covered in the DPAS Users Manual.

User Identification and Authentication. To gain access to DPAS, each user must be established with a unique logon ID, initial password, and site ID/database name. The Site Security Officers or Security Administrator at DECC-O will establish these items if no Site Security Officer exist at the site. This process will connect the logon ID to the required DPAS icons and programs. The Site Security Officer will provide a package to include the logon ID, initial password, site ID/database name, Network address, a list of icons and programs assigned, and the Security Awareness Guide to each DPAS user.

Logging on to DPAS. To gain access to DPAS:

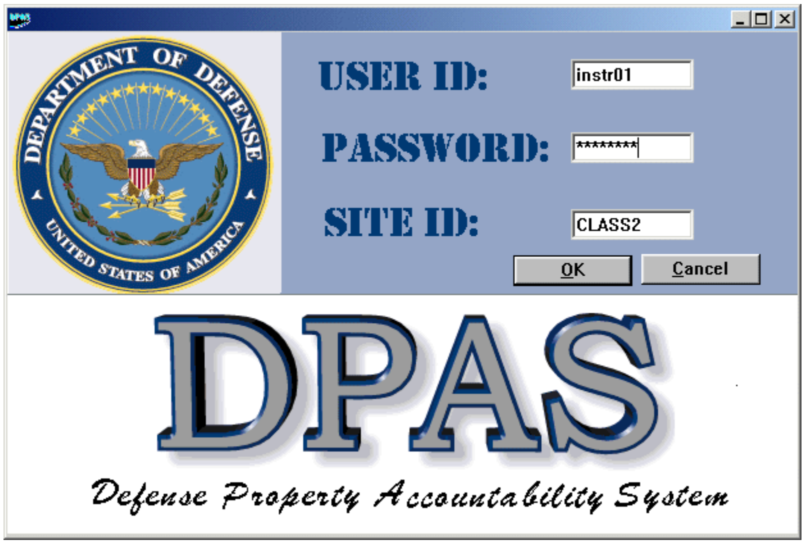
1. Click on the DPAS Icon from your desktop. You will be presented with the following screen, which means you have a successful connection. Click **OK.**



USE OF THIS OR ANY OTHER DEPARTMENT OF DEFENSE INTEREST COMPUTER SYSTEM (DODICS) CONSTITUTES YOUR CONSENT TO MONITORING BY DOD AUTHORIZED PERSONNEL FOR COMPUTER SECURITY AND SYSTEM MANAGEMENT PURPOSES. THIS DODICS AND ALL RELATED EQUIPMENT ARE TO BE USED FOR THE COMMUNICATIONS, TRANSMISSION, PROCESSING, MANIPULATION, AND STORAGE OF OFFICIAL U.S. GOVERNMENT OR OTHER AUTHORIZED INFORMATION ONLY. UNAUTHORIZED USE OF THIS COMPUTER MAY SUBJECT YOU TO CRIMINAL PROSECUTION AND PENALTIES.

2. At the LOGIN Screen, type the assigned **user ID** and press the **TAB** key.

3. Type the assigned **password**, then **TAB**. Type the Site ID, then press the **ENTER** key or click **OK.** An error message will be displayed if the user ID, password, or site ID/database name is incorrect. Correct the entry. Click **OK.**



USER ID: instr01

PASSWORD: ********

SITE ID: CLASS2

After three (3) unsuccessful attempts, a message will be displayed that says your account has been disabled. ***The password may need to be reset; follow local procedures for having the password reset***.

> **NOTE:**
> The password received with the LOGON ID is known as the initial password. This password must be changed in accordance with the rules in **User Security Responsibilities** prior to proceeding with DPAS. See **Password Change Procedures**. Anytime the password has been reset, it must be changed to something known only by the user. Passwords may be changed weekly if desired.

4. If the logon is successful, the DPAS Screen will be displayed.

5. The DPAS Main Menu and Desktop will be displayed. Select the desired icons by clicking on the appropriate icon, choosing from the drop down menu, or choosing the icon from the desktop.

6. If access is allowed, the corresponding program menu will be displayed. Select the desired program by clicking on your choice. If access to the module is not permitted, the icon will be grayed out. In addition, if access to certain programs within that module is not permitted, they will not appear on the drop down menu.

Password Change Procedures

1. Sign on to DPAS with LOGON ID, password, and Site ID.

2. From the DPAS Main Menu, select FILE/CHANGE USERS PASSWORD.

3. The screen will return with "Old Password". Type in the name of the old password. TAB to the "New Password" input box.

4. At the "New Password" input box, enter a new, personally derived password. Press the TAB key.

5. At the "New Password" input box, re-enter the new password. Press the ENTER key or click the SUBMIT button. This will verify the new password.

6. The DPAS Main Menu will be redisplayed. If the password change is successful, a message will appear that says "password change successful".

7. Error messages will be displayed if the NEW PASSWORD violates any of the rules outlined in **User Security Responsibilities**. The "New Password" prompt will be redisplayed.

8. After three (3) unsuccessful attempts, your account will be disabled.

Password Policies

1. The DPAS Security Administrator at the DECC-OD or the Site Security Officer will assign temporary passwords at the time end-user accounts are created.

2. End-users will be permitted to change their passwords at will, within the bounds of the restrictions identified, herein.

3. End-users will be required to change their passwords every 90 days.

4. Passwords must be changed any time they are compromised, possibly compromised, forgotten, or appear on a document.

5. End-users must wait five (5) days before changing their passwords again, without Security Administrator assistance.

6. Passwords will be a minimum of 8 and a maximum of 12 alphanumeric characters in length, must contain 2 of the following 3: a capital letter, a numeric or special character (only @, #, $, &, underscore). However, the first position cannot be an underscore.

7. Passwords will not contain any part of the end-users login ID, first name, last name, telephone number or e-mail address.

8. Passwords will not contain consecutively repeating characters.

9. DPAS will not permit end-users to reuse a password used within the last ten (10) password changes.

10. All passwords transmitted between DPAS client and server will be encrypted.

Logging Off of DPAS

To log off from a DPAS session:

1. From a program, click on CANCEL.

2. From the Main Menu, choose the red EXIT DPAS icon.

I&A Errors and Their Causes

While accessing DPAS, errors may occur at login time or during the session. The following table provides a list of error messages, a possible cause for the error, and recommended solutions.

I&A Error	**Possible Cause and Recommended Solution**
Login incorrect	The assigned logon ID was typed incorrectly, or the password is not valid. Retype the logon ID at the prompt (do not backspace), and the password at the Password input box. Press **RETURN** key.
Database – xxxxxxx-does not exist	The site ID/database name is incorrect. Enter the correct site ID/database name.
Invalid Entry	DPAS did not understand the entry. Re-enter the data.
User Id: xxxxxxxx Access to this program not authorized	User is not authorized to access the selected program or icons. Press **RETURN** to verify correctness of the program or icons being selected and retry entry.

Discretionary Access Controls

The ability to access DPAS icons and programs is controlled by the very nature of the duties assigned to the user. Access controls to read, update/delete is controlled at the program level. If the user has access to the program, then the user will be able to perform the actions associated with the program. The Information System Security Policy was developed to provide guidance to supervisors, Site Security Officers, and data owners for controlling accesses. The policy details by user class (i.e., Supply Clerk, Property Book Officer, Accountant, etc.) the icons and programs those positions are expected to access and maintain. While it is realized that some sites may only have a couple of users carrying out the responsibilities for property book management, DPAS is flexible enough to separate the duties among the user community regardless of the size. The DPAS Security icon provides to the Site Security Officer the ability to assign icons and programs to the user in a real-time environment.

Audit Trails

All changes to assets that change the database are subject to audit. Before and after images are maintained in a history file. The history file is accessible to users from the Inquiries icons from the DPAS Main Menu. This feature would allow a user to double check their work, or allow for tracking changes to an asset in the system. The DECC-O Security Administrator also has access to shell scripts to track user access events on the system.

Granting Security Access For A UIC

MODULE: Security

INTRODUCTION

This screen will allow your local Security Officer to add or delete an individual's login access for a specific UIC(s) and/or HRH Nbr(s) within an Accountable UIC group. Before your security officer can perform this function, the System Security Officer must assign the user a login ID to an Accountable UIC.

Your login ID can be assigned to multiple Accountable UICs, but you can only process transactions for the selected Accountable UIC.

Your DPAS Database Security Officer or Accountable UIC Security Officer can establish Accountable UICs on the database.

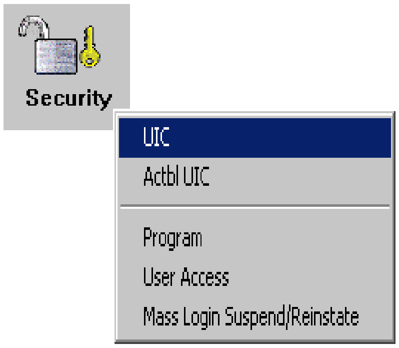
Once the Accountable UICs are established, your TASO/ISSO has the ability to add or delete login access to an Accountable UIC and add or delete login access to individual UICs for update purposes.

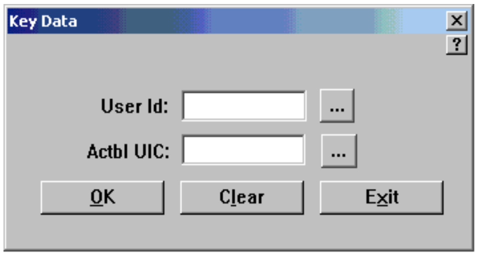
PREREQUISITES

None

STEPS TO PERFORM ACTION

1. Select the **Security** icon, or select **Security** from the menu bar.
2. Select **UIC** from the program group.

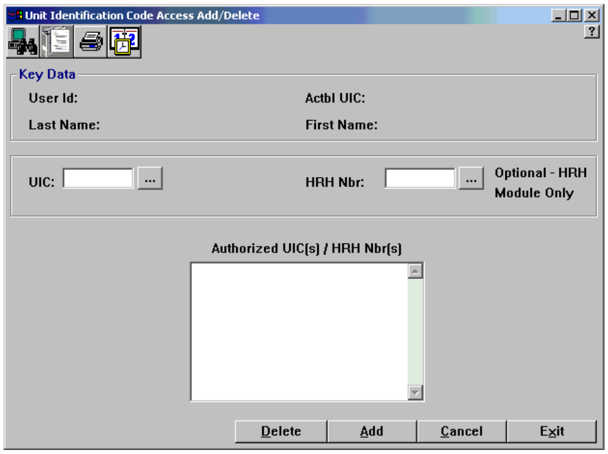




STEP 1:

a. **User Id:** Enter or browse for the user's DPAS login.
b. **Actbl UIC:** Enter or browse for the accountable UIC.
c. Click **OK**.

STEP 2:



a. **UIC:** Enter or browse for the UIC(s) to which access is to be added. You can multi-select UICs.

   CTRL+Click will let you randomly select UICs. **SHIFT+Click** will let you select UICs consecutively (they must be in order).

b. Click **Add**.

The UIC(s) will be added in the **Authorized UIC(s)/HRH Nbr(s)** window.

The Transaction Processed dialog box will be displayed.

c. Click **OK**.

d. Click **Exit**.

You are returned to the DPAS Main Menu.

Removing Access to UICs

1. Enter or browse for the user's DPAS login.
2. Enter or browse for the accountable UIC.
3. Click **OK**.
4. Enter or browse for the UIC(s) to be deleted. You can multi-select UIC(s).
5. Click **Delete**.

Granting Security Access For Hand Receipt Holders Only

MODULE: Security

INTRODUCTION

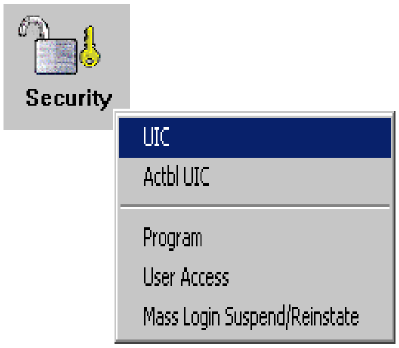
This process will show how to grant users access to the Hand Receipt Holder Module only.

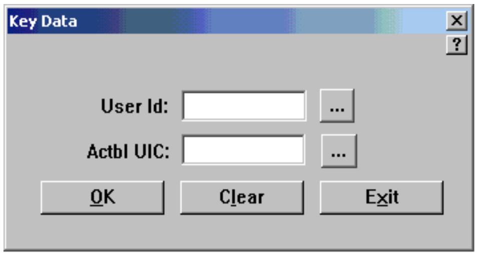
PREREQUISITES

None

STEPS TO PERFORM ACTION

1. Select the **Security** icon, or select **Security** from the menu bar.
2. Select **UIC** from the program group.

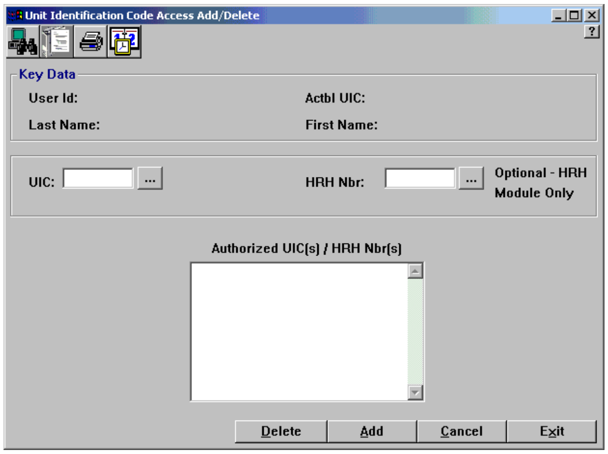




STEP 1:

a. **User Id:** Enter or browse for the user's DPAS login.
b. **Actbl UIC:** Enter or browse for the accountable UIC.
c. Click **OK**.

STEP 2:


Unit Identification Code Access Add/Delete
Key Data
User Id:
Actbl UIC:
Last Name:
First Name:
UIC:
HRH Nbr:
Optional - HRH Module Only
Authorized UIC(s) / HRH Nbr(s)
Delete
Add
Cancel
Exit

a. **UIC:** Enter or browse for the UIC to which the HRH Nbr is assigned.

b. **HRH Nbr:** Enter or browse for the HRH Nbr to which the user will have access. You can multi-select HRH Nbrs.

CTRL+Click will let you randomly select HRH Nbrs.
SHIFT+Click will let you select HRH Nbrs consecutively (they must be in order).

c. Click **Add**.

The UIC(s)/HRH Nbrs will be added in the **Authorized UIC(s)/HRH Nbr(s)** window.

The Transaction Processed dialog box will be displayed.

d. Click **OK**.

e. Click **Exit**.

You are returned to the DPAS Main Menu.

HINT!
If the user is to have access to the **Hand Receipt** module, then Security access for the HRH Nbr is not necessary. However, if the user is to have access to the **Hand Receipt Holder** module ***only***, then it is necessary to grant Security access to his HRH Nbr.

Removing Access to HRH Nbrs

1. Enter or browse for the user's DPAS login.
2. Enter or browse for the accountable UIC.
3. Click **OK**.
4. Enter or browse for the HRH Nbr(s) to be deleted. You can multi-select HRH Nbrs.
5. Click **Delete**.

Assigning Multiple Accountable UICs To A User

MODULE: Security

INTRODUCTION

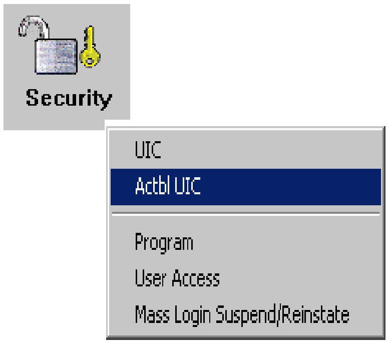
This process allows the ISSO the capability to assign users to multiple accountable UICs **after** DECC-O has established the Accountable UIC.

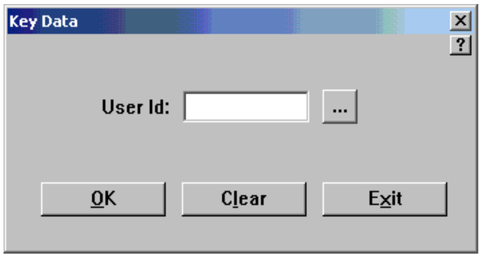
PREREQUISITES

None

STEPS TO PERFORM ACTION

1. Select the **Security** icon, or select **Security** from the menu bar.
2. Select **Actbl UIC** from the program group.

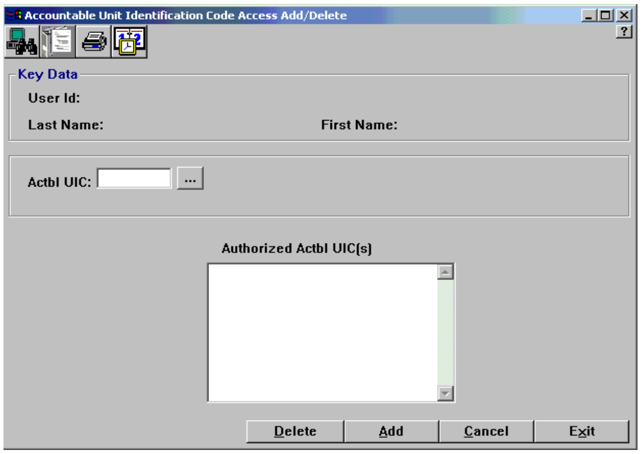




STEP 1:

a. **User Id:** Enter or browse for the user's DPAS log in id.
b. Click **OK**.

STEP 2:



a. **Actbl UIC:** Enter or browse for the Accountable UIC to which access is being given. You can multi-select UICs.

CTRL+Click will let you randomly select UICs.
SHIFT+Click will let you select UICs consecutively (they must be in order).

b. Click **Add**.

The Actbl UIC(s) will be added in the **Authorized Actbl UIC(s)** window.

The Transaction Processed dialog box will be displayed.

c. Click **OK**.

d. Click **Exit**.

You are returned to the DPAS Main Menu.

Removing Access to Accountable UIC(s)

1. Enter or browse for the user's DPAS login.
2. Click **OK**.
3. Enter or browse for the Actbl UIC(s) to be deleted. You can multi-select Actbl UICs.
4. Click **Delete**.

Modifying DPAS Program Access

MODULE: Security

INTRODUCTION

The purpose of this screen is to display the user's current permissions and provides the DPAS Coordinator the capability to change these permissions based on the user's requirements.

It also allows an ISSO the capability to copy a user's profile to other users.

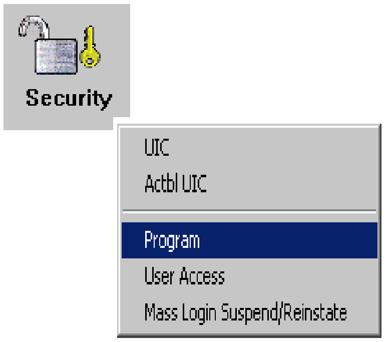
You will need to go into this process anytime there is a major release with new processes. DPAS does not give the users access to new processes.

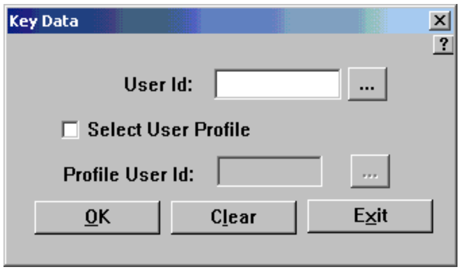
PREREQUISITES

None

STEPS TO PERFORM ACTION

1. Select the **Security** icon, or select **Security** from the menu bar.
2. Select **Program** from the program group.



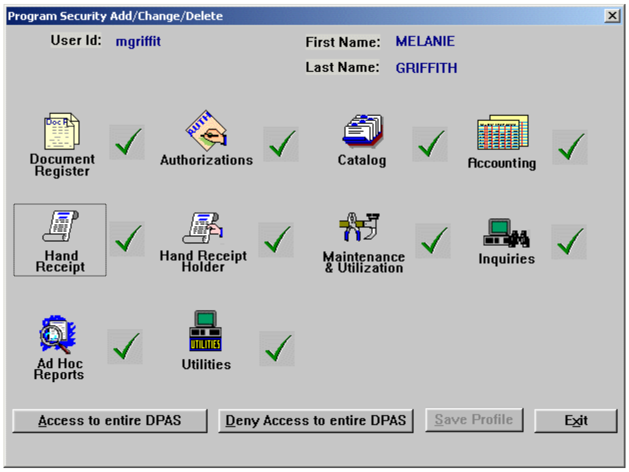


STEP 1:

a. **User Id:** Enter or browse for the user's DPAS login.
b. **Select User Profile:** Check this box if you want to use the profile from another user.
c. **Profile User Id:** If you checked the above box, enter or browse for the user id whose profile you will be using.
d. Click **OK**.

STEP 2:

a. Notice that the user's **User Id, First Name,** and **Last Name** is displayed.
b. Select the process to which you will be changing access.



Program Security Add/Change/Delete

User Id: mgriffit

First Name: MELANIE

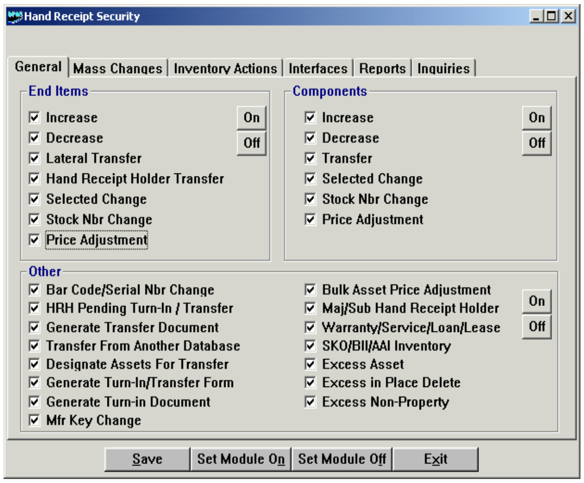
Last Name: GRIFFITH

HINT!

✓ The **Green Check** reflects which modules the user currently has permissions.

Access to entire DPAS will give the user access to all processes.

Deny Access to entire DPAS will deny the user access to all processes.



Hand Receipt Security

General | Mass Changes | Inventory Actions | Interfaces | Reports | Inquiries

End Items
- ☑ Increase
- ☑ Decrease
- ☑ Lateral Transfer
- ☑ Hand Receipt Holder Transfer
- ☑ Selected Change
- ☑ Stock Nbr Change
- ☑ Price Adjustment

Components
- ☑ Increase
- ☑ Decrease
- ☑ Transfer
- ☑ Selected Change
- ☑ Stock Nbr Change
- ☑ Price Adjustment

Other
- ☑ Bar Code/Serial Nbr Change
- ☑ HRH Pending Turn-In / Transfer
- ☑ Generate Transfer Document
- ☑ Transfer From Another Database
- ☑ Designate Assets For Transfer
- ☑ Generate Turn-In/Transfer Form
- ☑ Generate Turn-in Document
- ☑ Mfr Key Change
- ☑ Bulk Asset Price Adjustment
- ☑ Maj/Sub Hand Receipt Holder
- ☑ Warranty/Service/Loan/Lease
- ☑ SKO/BII/AAI Inventory
- ☑ Excess Asset
- ☑ Excess in Place Delete
- ☑ Excess Non-Property

STEP 3:

a. **Check/uncheck** individually to grant/deny access to a specific process.
b. Click on the tabs to display available menus with the module.
c. Use the **On/Off** buttons to grant/deny permissions to each of the defined group boxes.

HINT!

Set Module On will grant access to all processes within that module.

Set Module Off will deny access to all processes within that module.

Modifying DPAS User Access

MODULE: Security

INTRODUCTION

The purpose of this screen is to display the user's 1) current personal information, along with 2) a) database, b) report and c) inquiry access, and to provide 3) the DPAS Coordinator the capability to reset passwords.

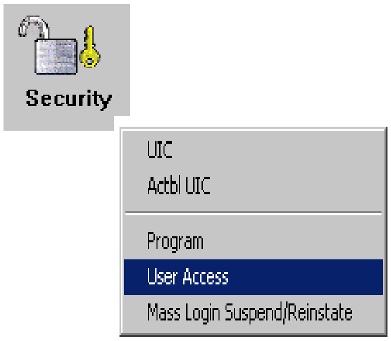
HINT!
If a user tries to acces DPAS and the login fails 3 times, DPAS will suspend the user's password. The ISSO will need to go into this process to reset the password.

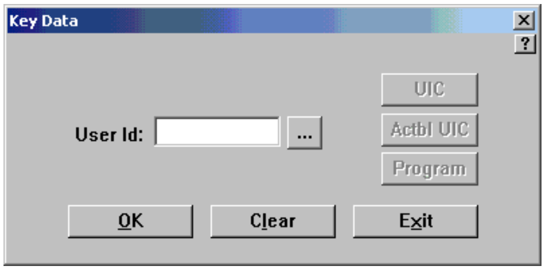
PREREQUISITES

None

STEPS TO PERFORM ACTION

1. Select the **Security** icon, or select **Security** from the menu bar.
2. Select **User Access** from the program group.

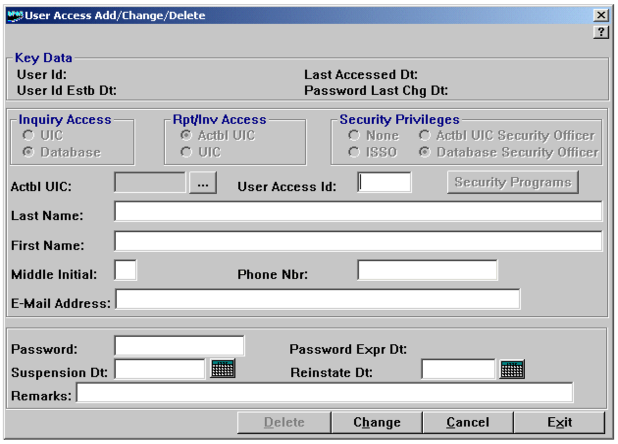




STEP 1:

a. **User Id:** Enter or browse for the user's login.
b. Click **OK**.

STEP 2:



Inquiry Access: ○ UIC ● Database

Rpt/Inv Access: ● Actbl UIC ○ UIC

Security Privileges: ○ None ○ ISSO ○ Actbl UIC Security Officer ● Database Security Officer

a. The **Inquiry Access, Rpt/Inv Access,** and **Security Privileges** group boxes are preset according to the users acceses level.
b. **Actbl UIC:** This field is preset.
c. **User Access Id:** These are locally assigned characters that uniquely identify a specific user.
d. **Last Name:** This is the last name of the user.
e. **First Name:** This is the first name of the user.
f. **Middle Initial:** This is the middle initial of the user.
g. **Phone Nbr:** This is the phone number of the user.
h. **E-Mail Address:** This is the e-mail address of the user.

HINT!

The **User Access Id, Last Name, First Name, Middle Initial, Phone Number** and **E-Mail Address** will tie records processed by the **User Id**.

i. **Password:** The ISSO can type in a temporary **Password** for the user, or leave blank. The ISSO will use this field to reset a user's password.
j. **Password Expr Dt:** This displays the date when the current password expired.
k. **Suspension Dt:** This is the date User Id was suspended for security violation, inactivity, etc.
l. **Reinstate Dt:** This is the date that a user who is currently suspended will be reinstated.
m. **Remarks:** Enter any remarks, if desired.
n. Click **Change**.

The Transaction Processed dialog box will be displayed.

o. Click **OK**.

You will be returned to the Key Data screen.

p. Click **Exit**.

Mass Login Suspend/Reinstate

MODULE: Security

INTRODUCTION

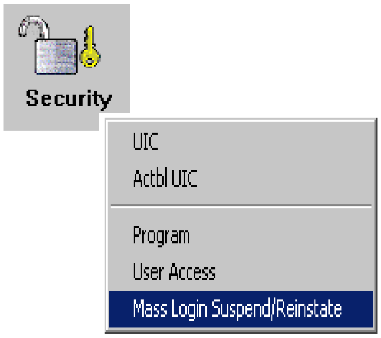
The purpose of this process is to allow users with security permission to suspend or reinstate users within DPAS. This process will allow the selected action to be taken either singularly or in mass. This process will update the Suspend and/or Reinstatement dates on the User Access Security table. This process will also add information to the Security History table, detailing all actions taken.

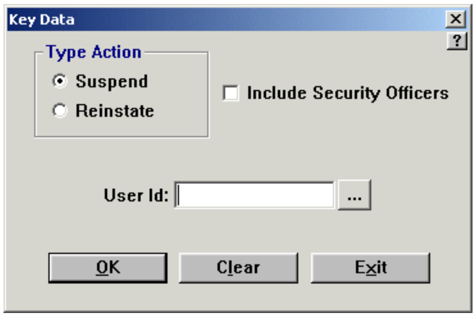
PREREQUISITES

None

STEPS TO PERFORM ACTION

1. Select the **Security** icon, or select **Security** from the menu bar.
2. Select **User Access** from the program group.





STEP 1:

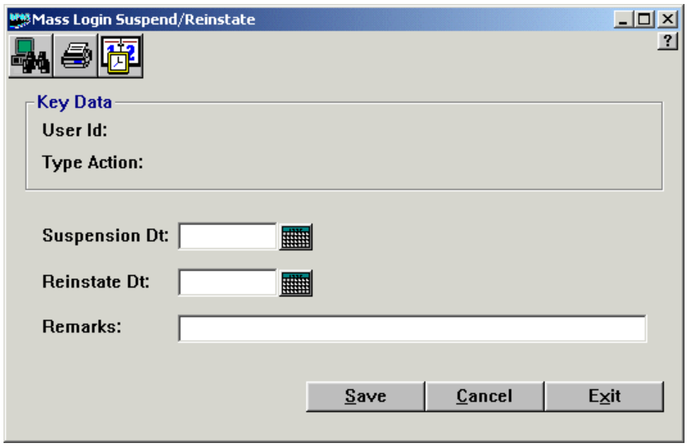
a. **Type Action:** Select the appropriate type of action.

Type Action	
Suspend	Click this button to perform the suspension from DPAS for the selected users.
Reinstate	Click this button to perform the reinstatement to DPAS for the selected users.

b. **Include Security Officers:** This checkbox indicates whether users at the same level of security are to be included in the action to be taken. Blank indicates do not include, checked indicates to include.

c. **User Id:** This field is initially populated with the User Id from User Defaults. You may change this by entering a value in the field. The User Id must exist on the User Access Security table. In addition, only those users at a lower security level will be displayed unless the Include Security Officers check-box is selected. In that case, users at the same security level will be displayed. Under no conditions can you suspend/reinstate users that are at a higher security level. The security levels are defined as follows, from the highest security level to the lowest security level: Database Security Officer, Accountable UIC Security Officer, ISSO (Information System Security Officer), None.
d. Click **OK**.

STEP 2:



a. **Suspension Dt:** This field is mandatory when the Type Action is "Suspend" and is not available when the Type Action is "Reinstate". The Suspension Date for the User ID selected will be initially displayed in this field, unless multiple users were selected; in that case the field will contain a value of 0. Enter or use the calendar button to select the date that the selected User IDs will be suspended. Date must be equal to or greater than the current system date.
b. **Reinstate Dt:** This field is mandatory when the Type Action is "Reinstate" and optional when the Type Action is "Suspend". The Reinstate Date for the User ID selected will be initially displayed in this field, unless multiple users were selected; in that case, the field will contain a value of 0. Enter or use the calendar button to select the date that the selected User IDs will be reinstated. Date must be equal to or greater than the current system date. When a Suspension Date of other than 0 is entered, the Reinstate Date must also be greater than the Suspension Date.
c. **Remarks:** This field is mandatory. Remarks must be entered detailing the reason for the action.
d. Click **Save**.

The Transaction Processed dialog box will be displayed.

e. Click **OK**.

You will be returned to the Key Data screen.

f. Click **Exit**.

Terms and Definitions

Audit Trail. A chronological record of system activities that is sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results.

Authentication. Verification of a user, device, or entity in an AIS prior to allowing access to the system resource.

Authorization. Granting access rights to users, processes, and programs by responsible administrator.

Automated Information System (AIS). An assembly of computer hardware, software and/or firmware configured to collect, create, communicate, disseminate, process, store, and/or control data or information.

AIS Security. Measures and controls that protect an AIS against denial of service and unauthorized (accidental or intentional) disclosure, modification, or destruction of AISs and data. AIS security includes consideration of all hardware and/or software functions.

Availability. The state when AIS resources are in the place needed by the user at the time the user needs them and in the form the user requires.

Communications Security. A combination of technical measures designed to protect confidentially, integrity and availability of information while being transmitted on a telecommunications system. Communications Security includes crypt security, transmission security, and physical security of communications security material and information.

Confidentiality. An aspect of security that deals with the restriction of information to only those who are authorized to use it and have legitimate "need-to-know".

Controlled Access Protection. Access control through logon procedures, audit of security-relevant events, and resource isolation.

Database Name. A unique name assigned to an activity's physical database.

Data Confidentiality. Data confidentiality provides the protection of information from unauthorized disclosure.

Data Integrity. The state that exists when computerized data is the same as the source documents and has not been exposed to accidental or malicious alteration or destruction.

Denial of Service. Any action that prevents any part of an AIS from functioning in accordance with it intended purpose.

Discretionary Access Control (DAC). A means of restricting access to AIS information (object) based on the identity and need to know of the user, process and/or group.

Designated Approving Authority (DAA). The official who has the authority to decide on accepting the security safeguards prescribed for an AIS or the official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards.

DPAS. Defense Property Accountability System. DPAS provides a standardized database management system to assure the accountability of an activity's property.

Hand Receipt Holder. Person(s) designated in writing and located at the field operating unit level having physical custody and control over property. This person is responsible for keeping the property records for their area of responsibility, taking and maintaining inventories, informing the property office of all new items of accountable property acquired as well as old items of accountable property to be excessed or removed.

Help Desk. The Help Desk resides at the Program Management Support Office (PMSO) DFAS Columbus and is a 24-hour, 7 day a week support service for the DPAS users. The Help Desk is responsible for recording and tracking the status of DPAS user problems as well as resolving DPAS user problems. See Appendix B for security responsibilities.

Icons. A term used to identify a function within DPAS (e.g., Document Register, Authorization, Catalog, etc.). Synonymous with "compartment". Users having a specific "need to know" will be assigned to multiple icons/compartments depending on their duties.

Identification. The process that enable recognition of a user or process by a system.

Information System Security Officer (IAO). The person responsible to the DAA for ensuring that security is provided for and implemented throughout the life cycle of an AIS.

Local Area Network (LAN). A collection of computing and communications devices connected via a common transmission media and deployed in a s small geographic area such as an office, building, or campus.

Logon ID. A unique 6 to 8 character identifier assigned to the user.

Password. A unique 8 to 12 character identifier known only to the user, when used in combination with the logon ID, will allow the user to sign on to the DPAS.

Physical Security. The application of physical barriers and control procedures as preventive measures against threats to AIS resources, information, and facilities.

Programs. A term used to identify functions within icons (i.e., within Document Register is Request for Issue, Request for Miscellaneous Actions, etc.) Users responsible for creating the Document Register may have access to any/or all of the programs within the icons as determined by their duties.

Property. Anything that may be owned. Property includes real property and personal property.

Property Accountability. Property accountability includes responsibilities for such tasks as tracking the movement of assets, recording changes in physical condition, and verification of physical counts. Property managers exercise this responsibility and maintain proper control over an organization's assets through record keeping, effective policies and procedures and appropriate security controls.

Property, Plant and Equipment. Tangible assets, including land, that meet the following criteria:

- They have estimated useful lives of 2 years or more
- They are not intended for sale in the ordinary course of operations; and
- They have been acquired or constructed with the intention of being used, or being available for use by the entity.

Reliability. The quality of producing the same results each time the same procedure and products are used, usually implying dependable equipment and bug-free processing routines.

Safeguards. An implementation of technology or techniques to protect confidentiality, integrity, and availability.

Security Policy. The set of laws, rules, practices, and procedures, which regulate how an organization manages, protects, and distributes sensitive information and AIS.

Sensitive Information. Any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the conduct of business or the privacy to which individuals are entitled under section 552a or Title 5, United States Code (Privacy Act).

Site ID. Term used interchangeable with database name.

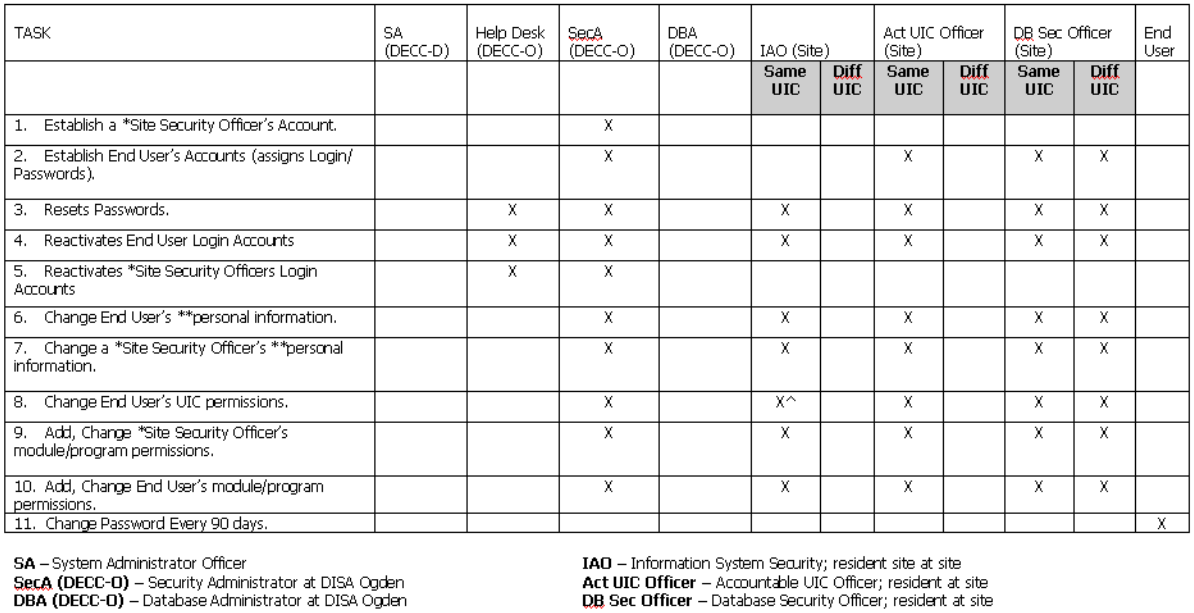
System Administrator. The person responsible for the installation, operation, maintenance, and performance of the DPAS Servers.

User. A person or process authorized to access and interact directly with a computer system.

Wide Area Network (WAN). A collection of computing and communications devices, including LANs, connected via a variety of transmission media, including telephone lines and other public networks, across a broad geographic area.

Security Responsibility Table

* Site Security Officer (site) – IAO, Act UIC, Officer, DB Sec Officer
** Personal Information – name, phone number, e-mail address
^ The IAO can only assign UIC to users that have the same UIC as his/hers



TASK	SA (DECC-D)	Help Desk (DECC-O)	SecA (DECC-O)	DBA (DECC-O)	IAO (Site)		Act UIC Officer (Site)		DB Sec Officer (Site)		End User
					Same UIC	**Diff UIC**	**Same UIC**	**Diff UIC**	**Same UIC**	**Diff UIC**	
1. Establish a *Site Security Officer's Account.			X								
2. Establish End User's Accounts (assigns Login/ Passwords).			X				X		X	X	
3. Resets Passwords.		X	X		X		X		X	X	
4. Reactivates End User Login Accounts		X	X		X		X		X	X	
5. Reactivates *Site Security Officers Login Accounts		X	X								
6. Change End User's **personal information.			X		X		X		X	X	
7. Change a *Site Security Officer's **personal information.			X		X		X		X	X	
8. Change End User's UIC permissions.			X		X^		X		X	X	
9. Add, Change *Site Security Officer's module/program permissions.			X		X		X		X	X	
10. Add, Change End User's module/program permissions.			X		X		X		X	X	
11. Change Password Every 90 days.											X

SA – System Administrator Officer
SecA (DECC-O) – Security Administrator at DISA Ogden
DBA (DECC-O) – Database Administrator at DISA Ogden

IAO – Information System Security; resident site at site
Act UIC Officer – Accountable UIC Officer; resident at site
DB Sec Officer – Database Security Officer; resident at site

Security Personnel Access Status

Access Status	SA (DECC-D)	SecA (DECC-O)	DBA (DECC-O)	IAO (Site)	Act UIC Officer (Site)	DB Sec Officer (Site)	End User
1. Has a UNIX account	X		X				
2. Has access to CRON processes	X		X				
3. Has access to auditing/accounting data	X		X				X
4. Can Startup and shutdown processes	X		X				
5. Has a DPAS account				X	X	X	X